CLAIMS

1. An authentication intrusion detection system responsive to an attempted intrusion into a local computer system to which access is gained by prospective users entering a personal identifier followed by a secret authenticator, said authentication intrusion detection system comprising:

a local computer system authenticator file communicating with said local computer system and having stored therein the secret authenticators corresponding to the personal identifiers entered by prospective users;

an authenticator broker system to intercept and redirect the identifier and secret authenticator of a prospective user from the local computer system;

an authenticator broker file communicating with said authenticator broker system and having stored therein the secret authenticators corresponding to the personal identifiers entered by the prospective users at the local computer system and stored in the local computer system authenticator file, whereby a prospective user can gain access to the local computer system when the authenticator entered by the prospective user matches the authenticator stored in said authenticator broker file; and

a decoy authenticator file communicating with the authenticator broker system to assign a decoy authenticator for the secret authenticator entered by the prospective user at the local computer system and stored in the local computer system authenticator file.

2. The authentication intrusion detection system recited in Claim 1, wherein said decoy authenticator file is a mapping file.

3. The authentication intrusion detection system recited in Claim 2, wherein a replacement identifier is randomly assigned by said mapping file for the identifier entered by the prospective user and intercepted by said authenticator broker system.

4. The authentication intrusion detection system recited in Claim 3, wherein said replacement identifier assigned by said mapping file for the identifier entered by the prospective user and intercepted by said authenticator broker system is unique to the prospective user.

5. The authentication intrusion detection system recited in Claim 2, wherein said replacement identifier assigned by said mapping file for the identifier entered by the prospective user and intercepted by said authenticator broker system is unknown to the prospective user.

6. The authentication intrusion detection system recited in Claim 1, wherein said authenticator broker system is a host computer that is responsive to the prospective user's attempt to gain access to the local computer system and to any intrusion into the local computer system.

7. The authentication intrusion detection system recited in Claim 6, wherein said host computer is a mainframe computer.

8. The authentication intrusion detection system recited in Claim 7, further comprising a mapping file communicating with the authenticator broker system to assign a replacement

identifier stored in said mapping file for the identifier entered by the prospective user at the local computer system and intercepted by said authenticator broker system, said authenticator broker system, said mapping file and said decoy authenticator file being located at said mainframe host computer.

9. A method for detecting a compromise by an intruder to a local computer system that requires authorized users to log onto the local computer system by means of successfully entering a personal identifier and a secret authenticator for purposes of user authentication, said method comprising the steps of:

intercepting the secret authenticator entered by the authorized user at the local computer system and forwarding the secret authenticator to an authenticator broker system;

transmitting from the authenticator broker system to the local computer system a decoy password in substitution of the secret authenticator of the authorized user; and

logging the authorized user onto the local computer system on the basis of the decoy password transmitted to the local computer system from the authenticator broker system;

whereby an intruder who breaks into the local computer system will capture and enter the authorized user's personal identifier and the decoy password substituted for the authorized user's secret authenticator to be forwarded to the authenticator broker system by which to provide an indication that the local computer system has been compromised.

10. The method recited in Claim 9, including the additional step of storing the decoy password in an authenticator file of each of said local computer system and said authenticator broker system.

11. The method recited in Claim 9, including the additional step of maintaining the decoy password in secrecy from the authorized user.

12. The method recited in Claim 9, in which the user accesses a plurality of local computer systems, each local system being identified in an identifier mapped to each decoy and authenticator, and wherein the identification of a compromised system is determined by the local system identifier.